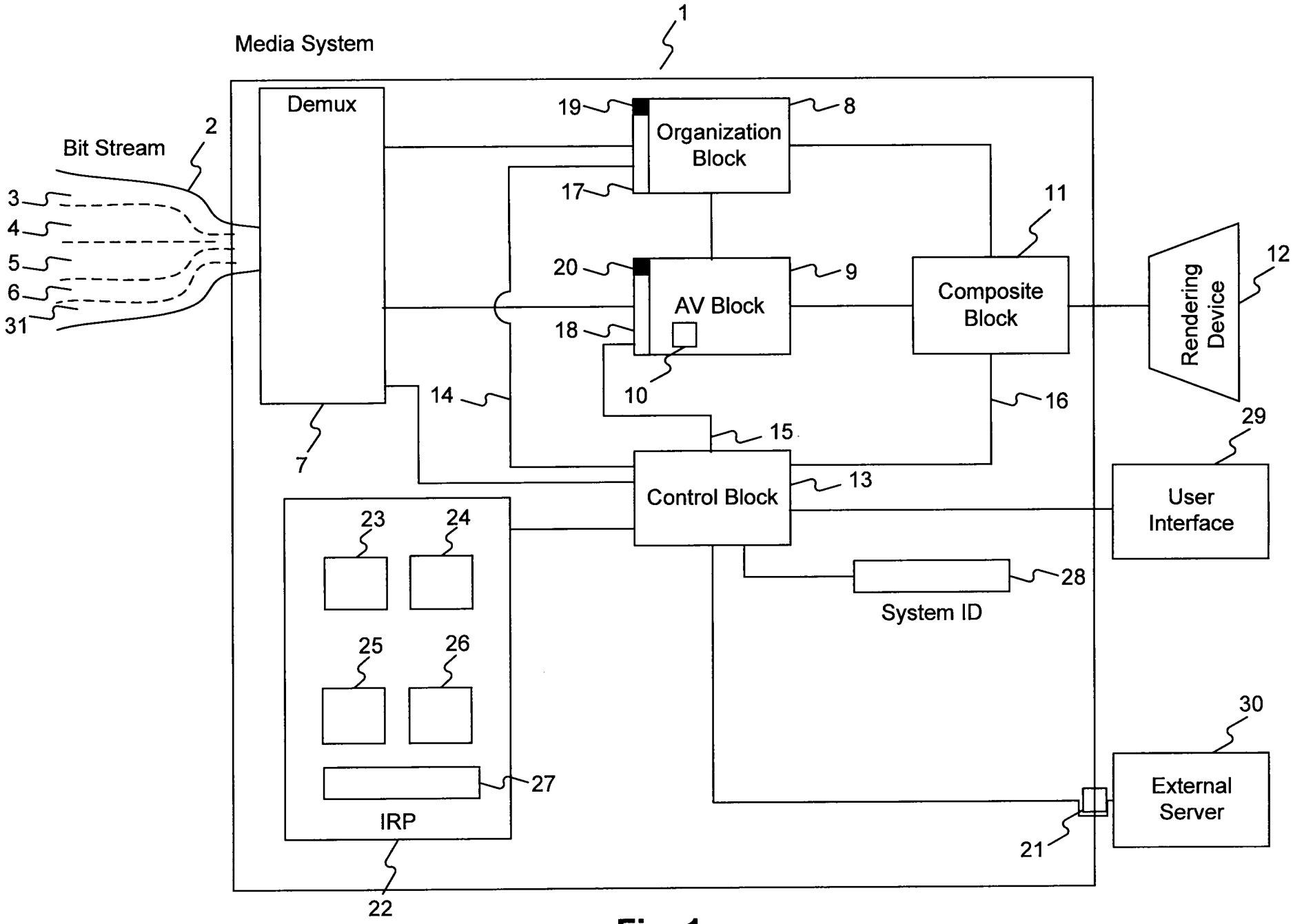

Media System
1
Demux
Bit Stream
2
3
4
5
6
31
19
Organization Block
8
17
11
20
AV Block
9
Composite Block
12
Rendering Device
18
10
14
16
15
7
29
Control Block
13
User Interface
23
24
25
26
28
System ID
27
IRP
22
30
External Server
21

Fig. 1

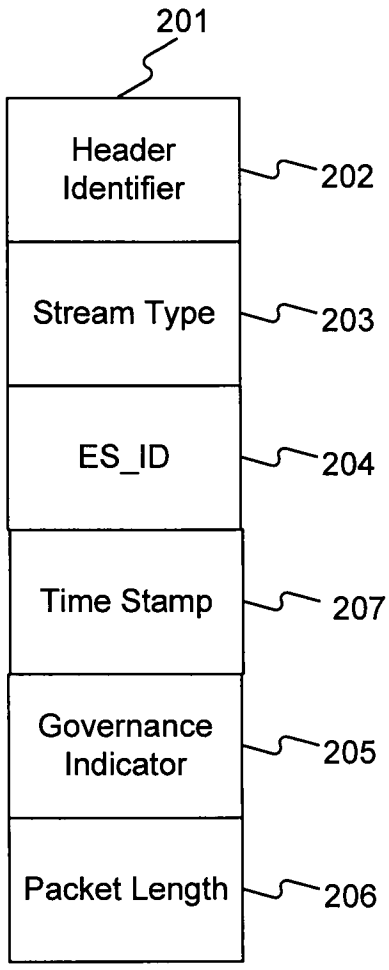

201
Header Identifier
202
Stream Type
203
ES_ID
204
Time Stamp
207
Governance Indicator
205
Packet Length
206

**Fig. 2**

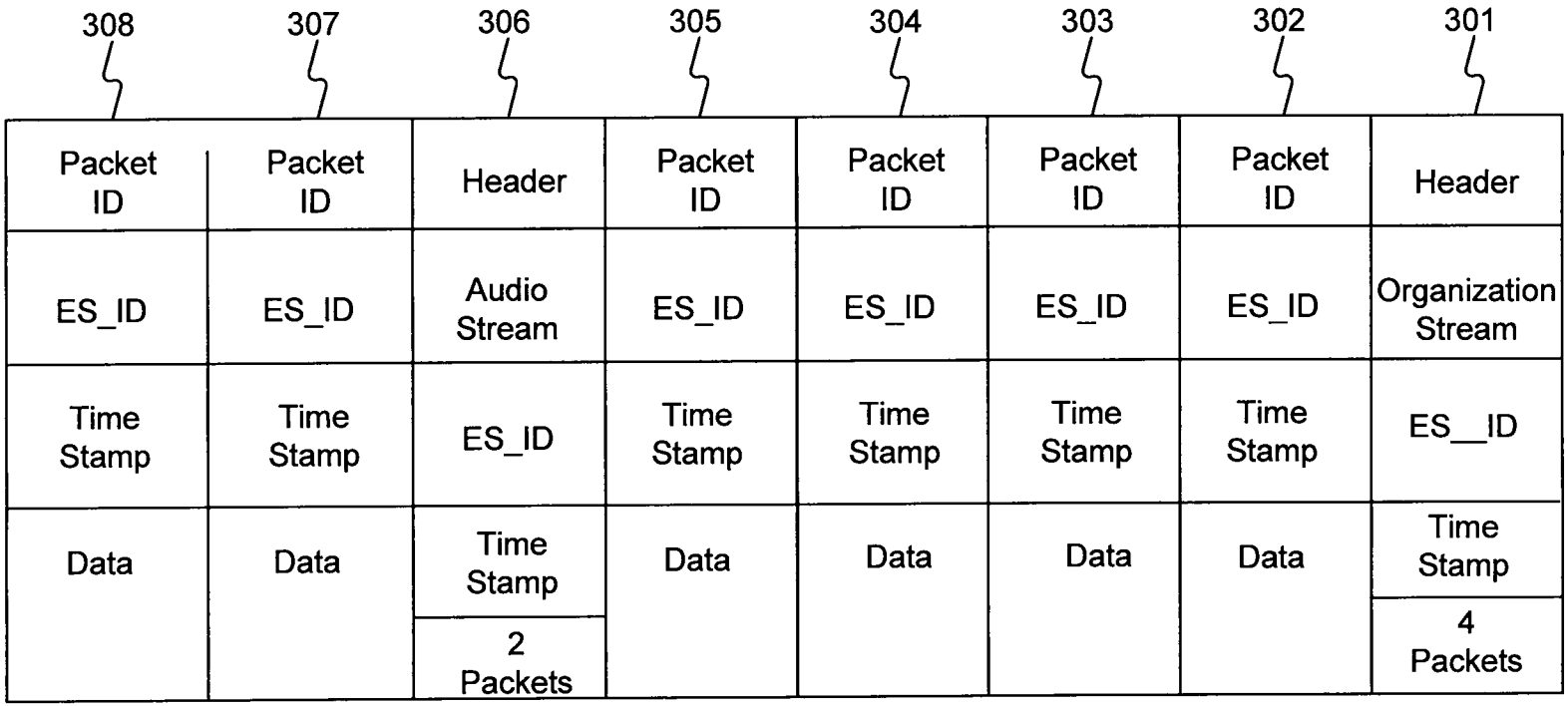

308
307
306
305
304
303
302
301
Packet ID
Packet ID
Header
Packet ID
Packet ID
Packet ID
Packet ID
Header
ES_ID
ES_ID
Audio Stream
ES_ID
ES_ID
ES_ID
ES_ID
Organization Stream
Time Stamp
Time Stamp
ES_ID
Time Stamp
Time Stamp
Time Stamp
Time Stamp
ES__ID
Data
Data
Time Stamp
Data
Data
Data
Data
Time Stamp
2 Packets
4 Packets

**Fig. 3**

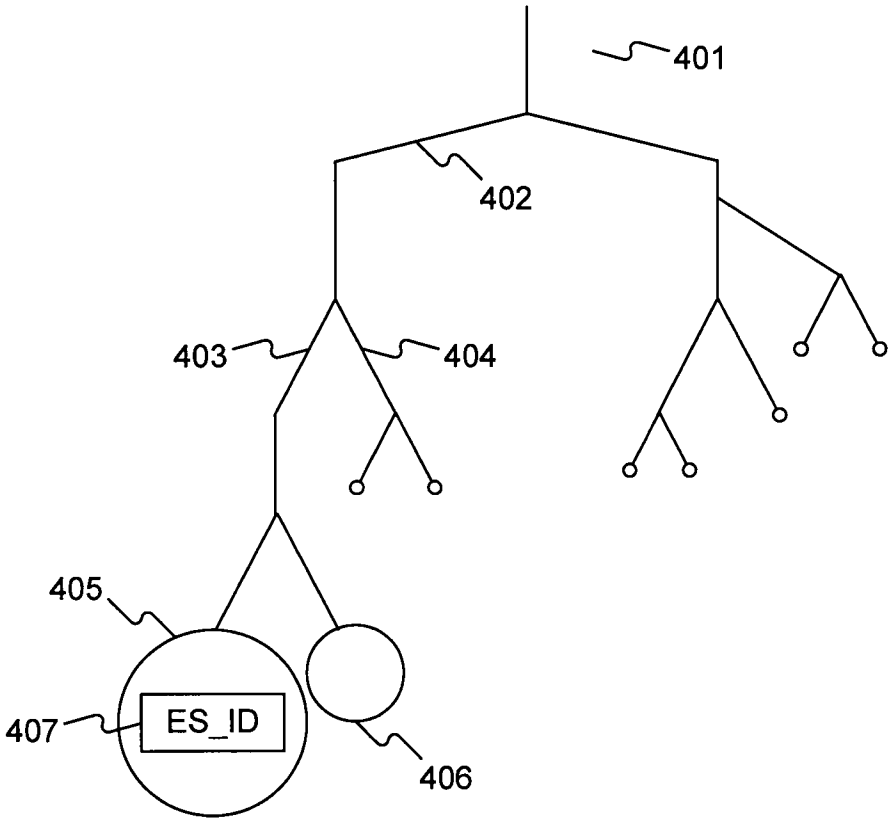



**Fig. 4**

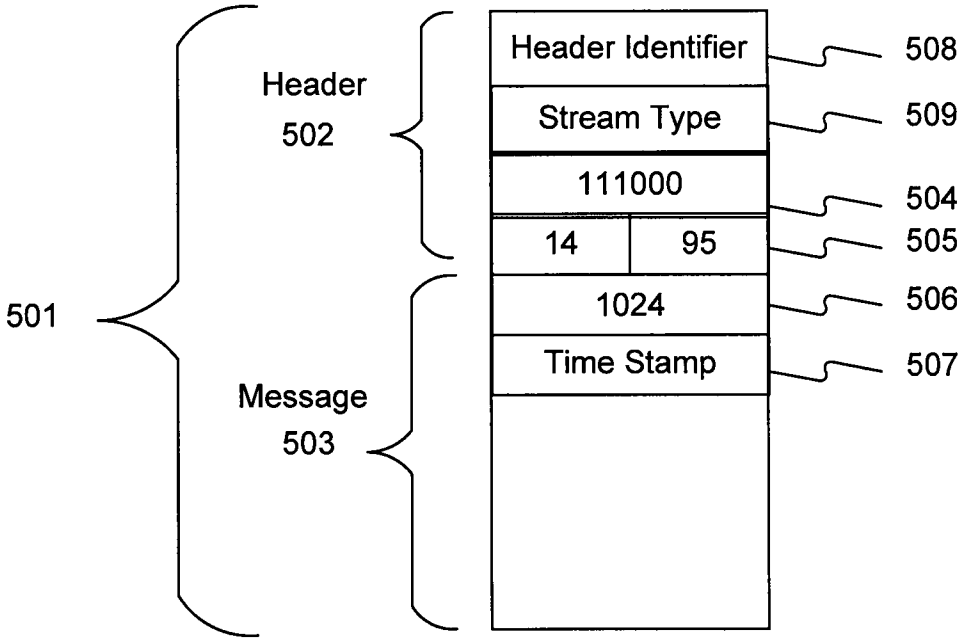

Control Message
501
Header
502
Message
503
Header Identifier
Stream Type
111000
14
95
1024
Time Stamp
508
509
504
505
506
507

Fig. 5

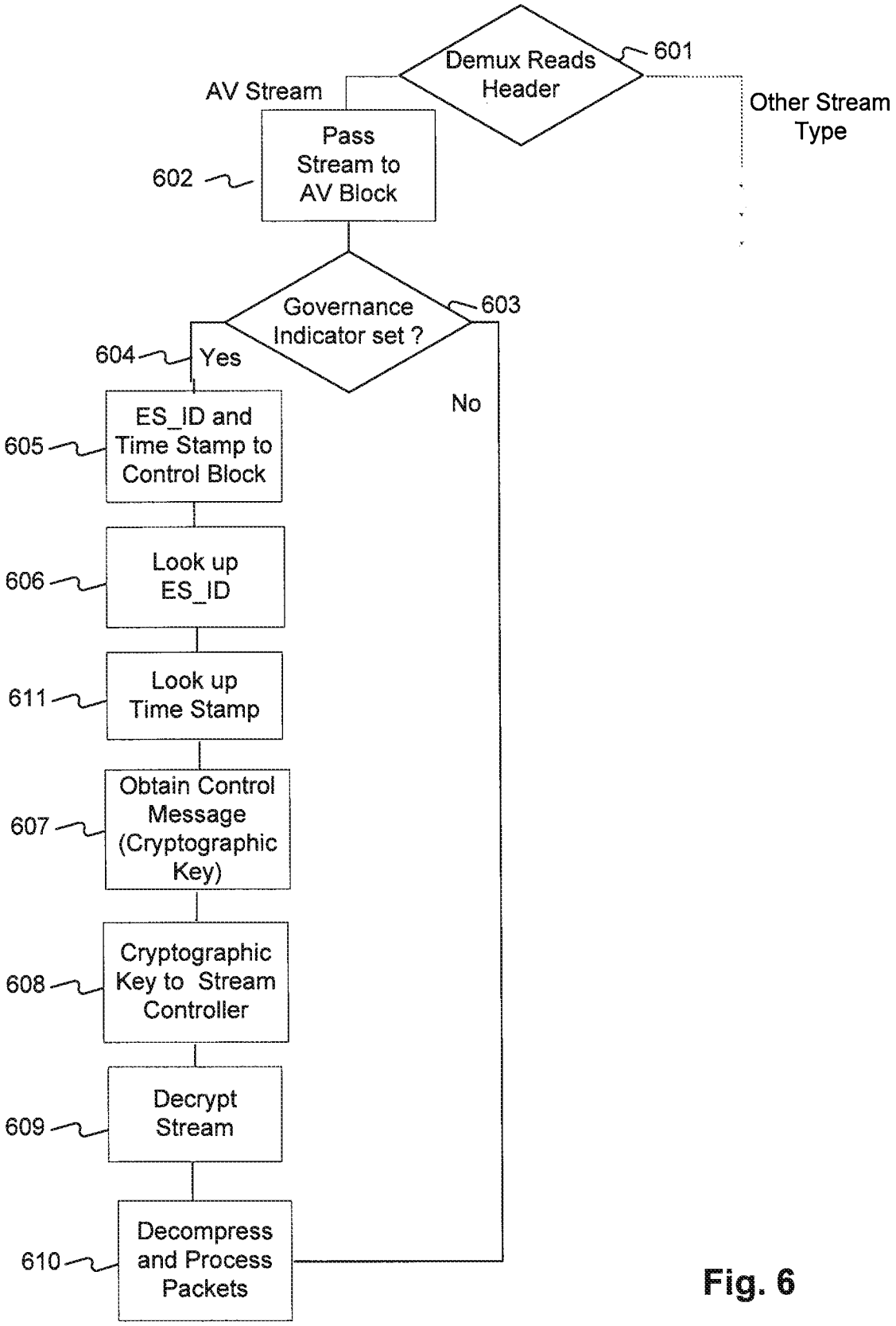

Demux Reads Header
601
AV Stream
Other Stream Type
Pass Stream to AV Block
602
Governance Indicator set ?
603
604
Yes
No
ES_ID and Time Stamp to Control Block
605
Look up ES_ID
606
Look up Time Stamp
611
Obtain Control Message (Cryptographic Key)
607
Cryptographic Key to Stream Controller
608
Decrypt Stream
609
Decompress and Process Packets
610

Fig. 6

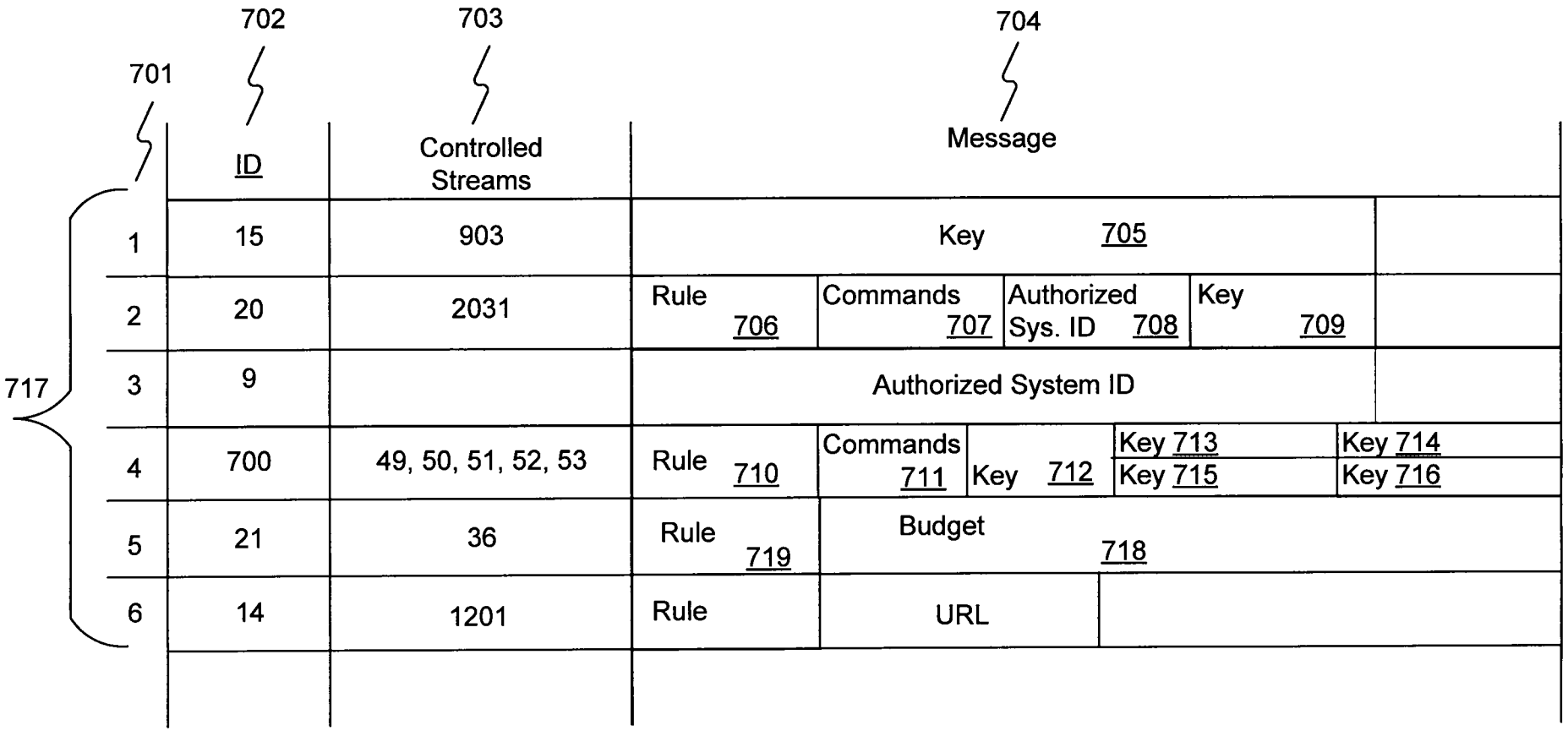

701
702
703
704
ID
Controlled Streams
Message
717
1
15
903
Key 705
2
20
2031
Rule 706
Commands 707
Authorized Sys. ID 708
Key 709
3
9
Authorized System ID
4
700
49, 50, 51, 52, 53
Rule 710
Commands 711
Key 712
Key 713
Key 714
Key 715
Key 716
5
21
36
Rule 719
Budget 718
6
14
1201
Rule
URL

Fig. 7

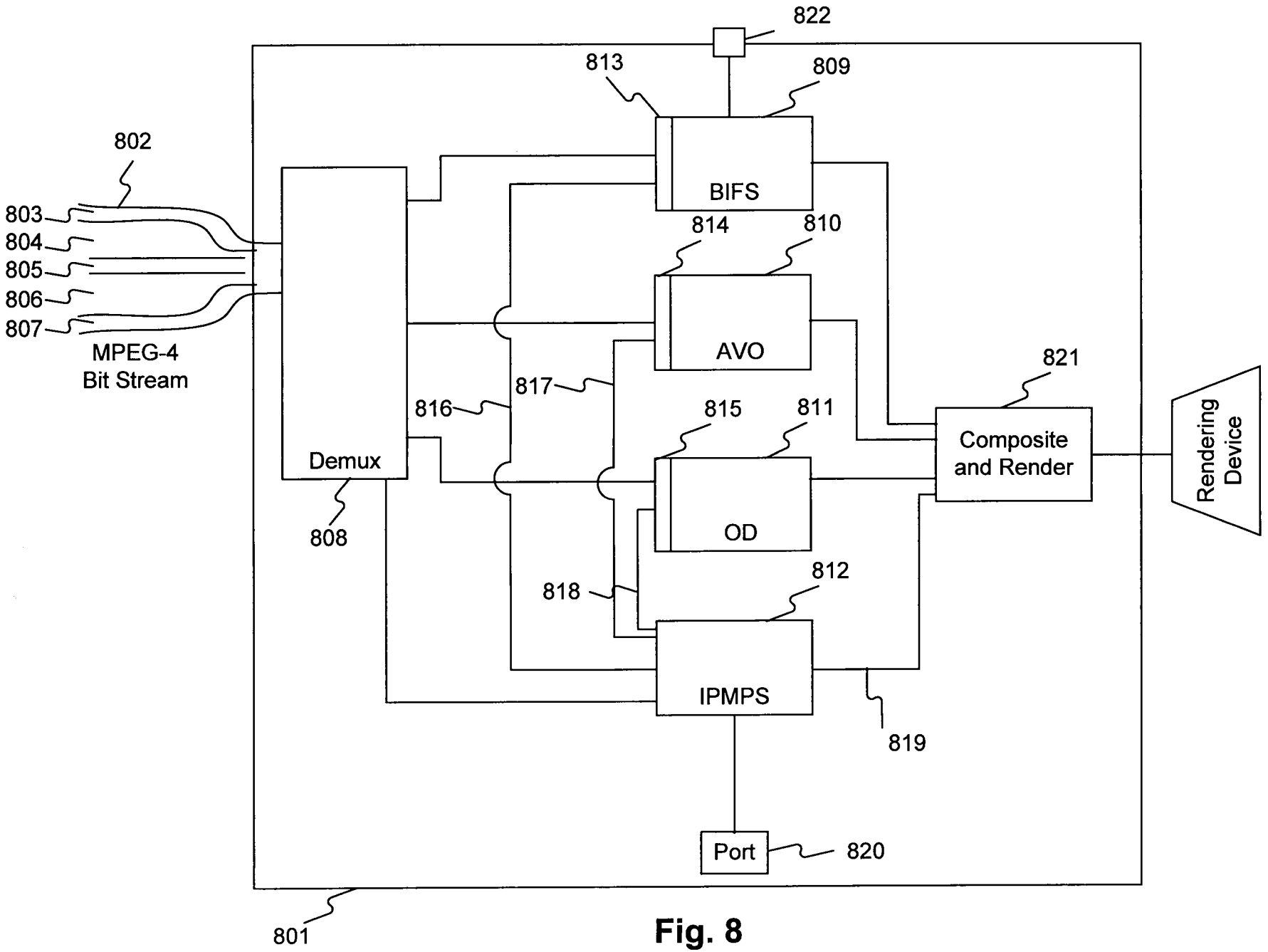

822
813
809
802
803
804
805
806
807
MPEG-4
Bit Stream
BIFS
814
810
AVO
821
817
816
815
811
Demux
Composite
and Render
Rendering
Device
OD
808
812
818
IPMPS
819
Port
820
801

Fig. 8

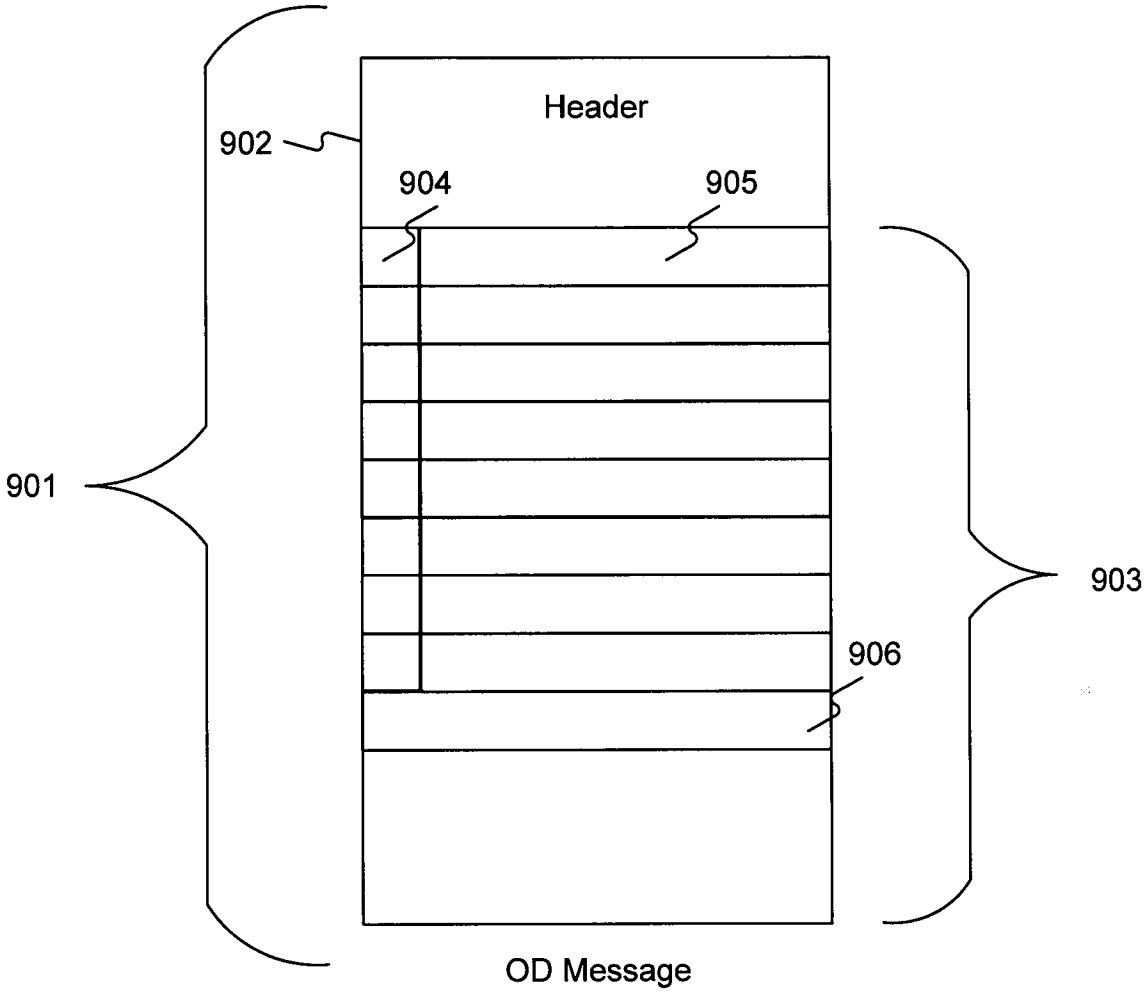



**Fig. 9**

**IPMP Table**

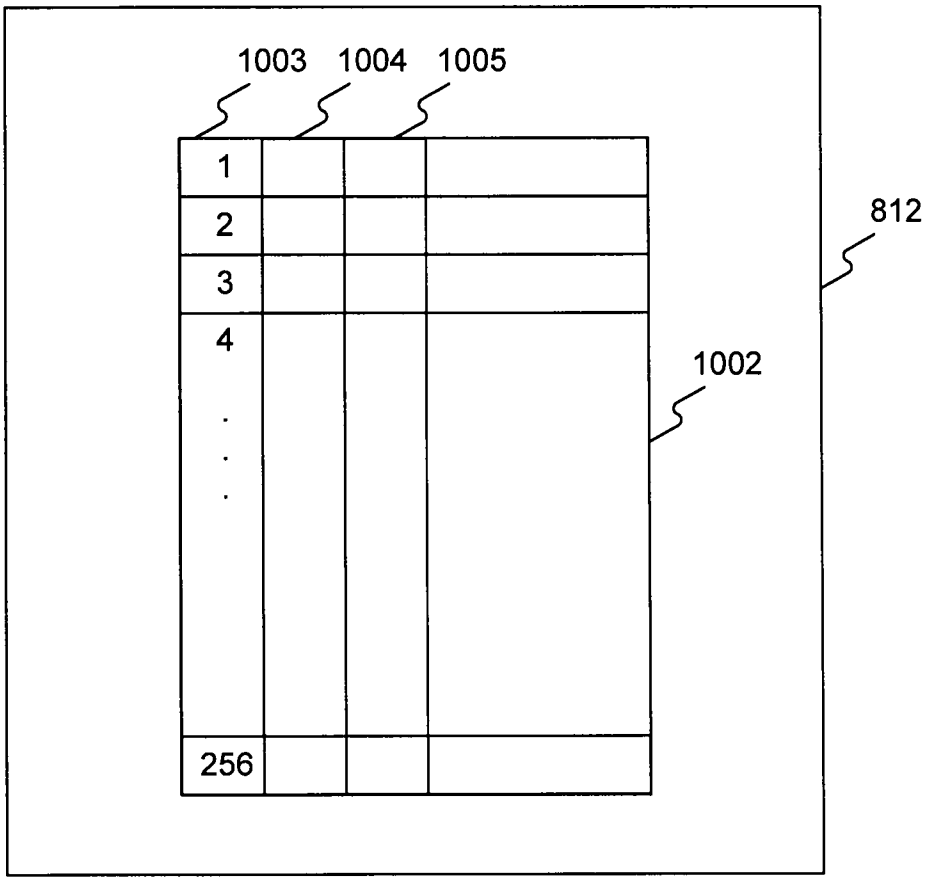



**Fig. 10**

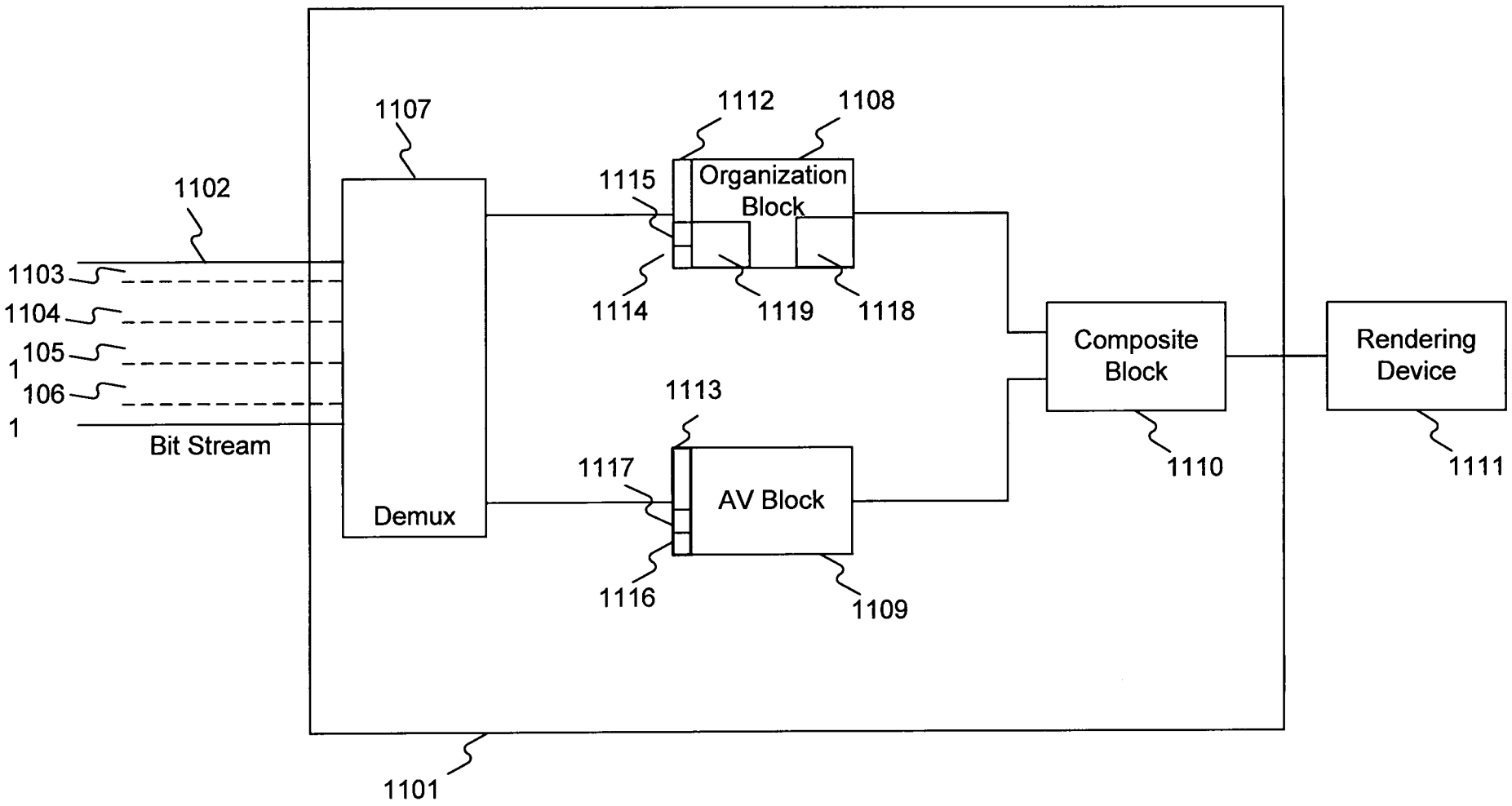

1107
1112
1108
1102
1115
Organization Block
1103
1104
1105
1
106
1
Bit Stream
1114
1119
1118
Composite Block
Rendering Device
1113
1117
AV Block
Demux
1110
1111
1116
1109
1101

**Fig. 11**

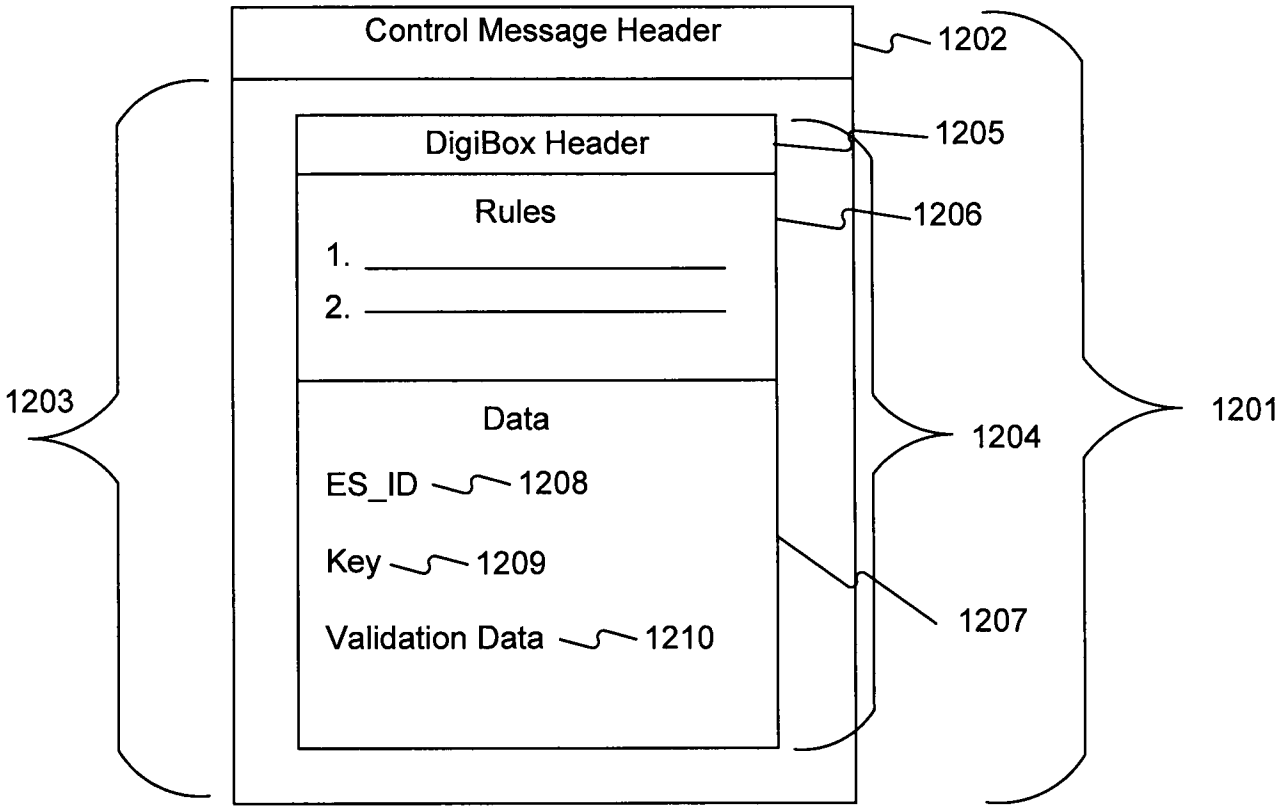

Control Message Header
1202
DigiBox Header
1205
Rules
1206
1.
2.
1203
Data
1204
1201
ES_ID
1208
Key
1209
1207
Validation Data
1210

Fig. 12

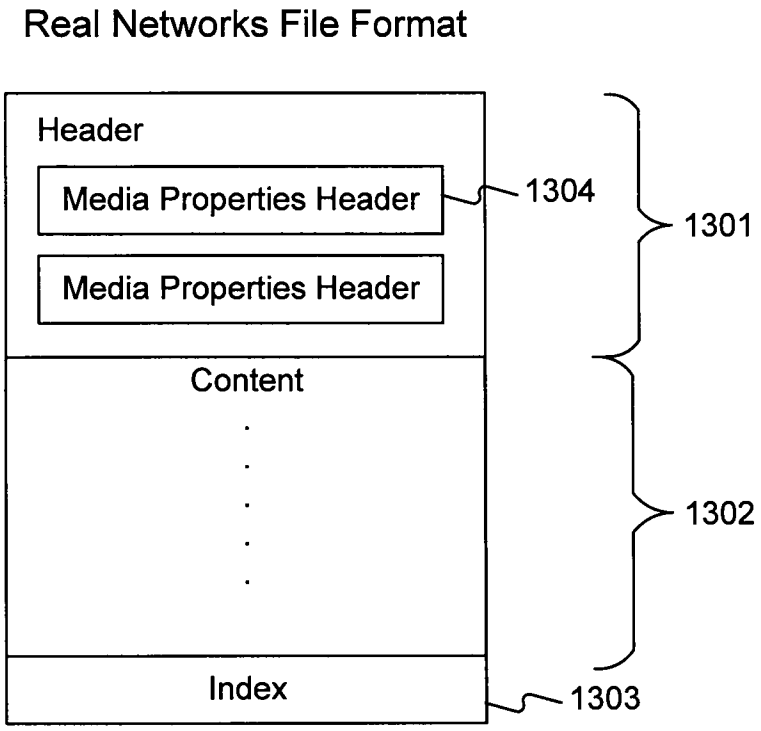

Real Networks File Format
Header
Media Properties Header
Media Properties Header
1304
1301
Content
1302
Index
1303

**Fig. 13**

Real Networks/Protected File Format

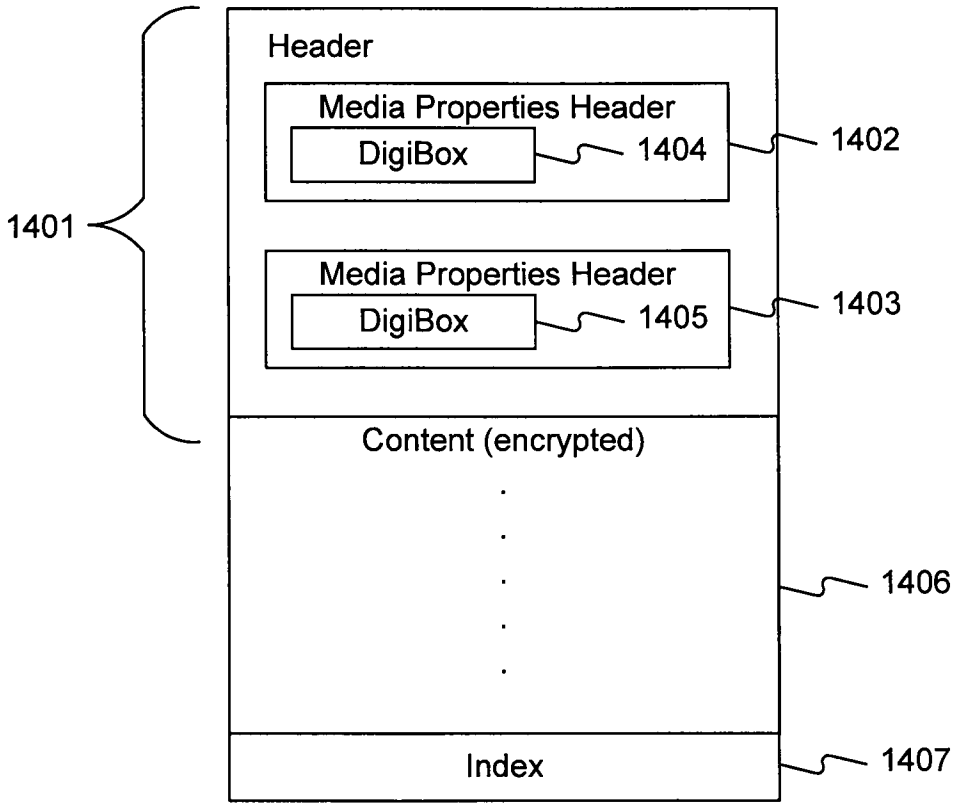



**Fig. 14**

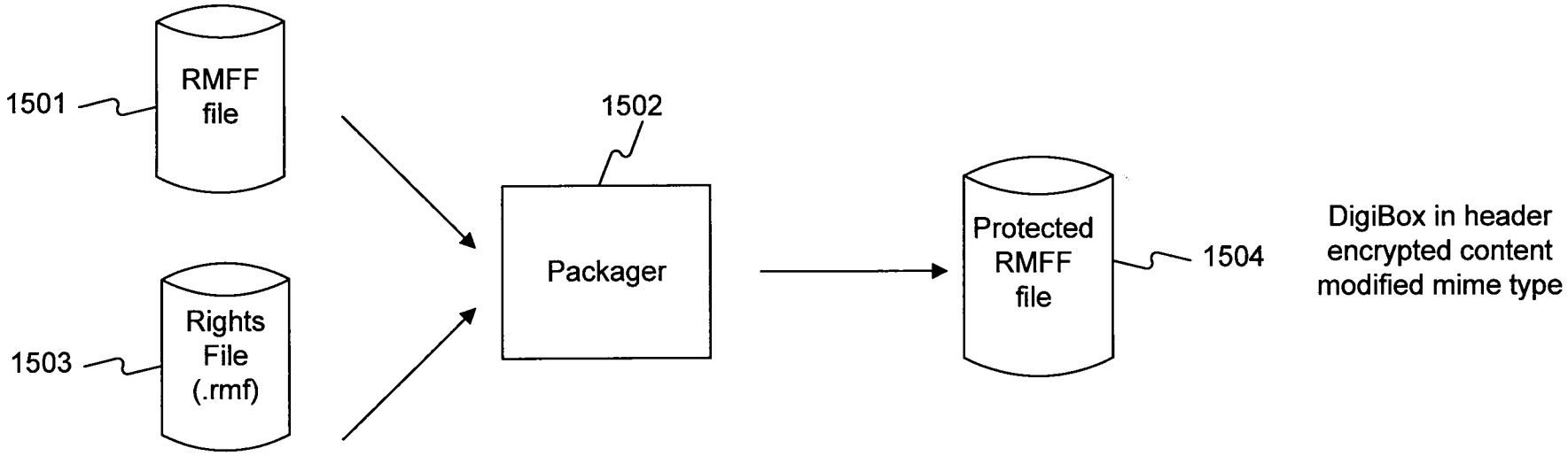

1501
RMFF file
1503
Rights File (.rmf)
1502
Packager
Protected RMFF file
1504
DigiBox in header
encrypted content
modified mime type

Fig. 15

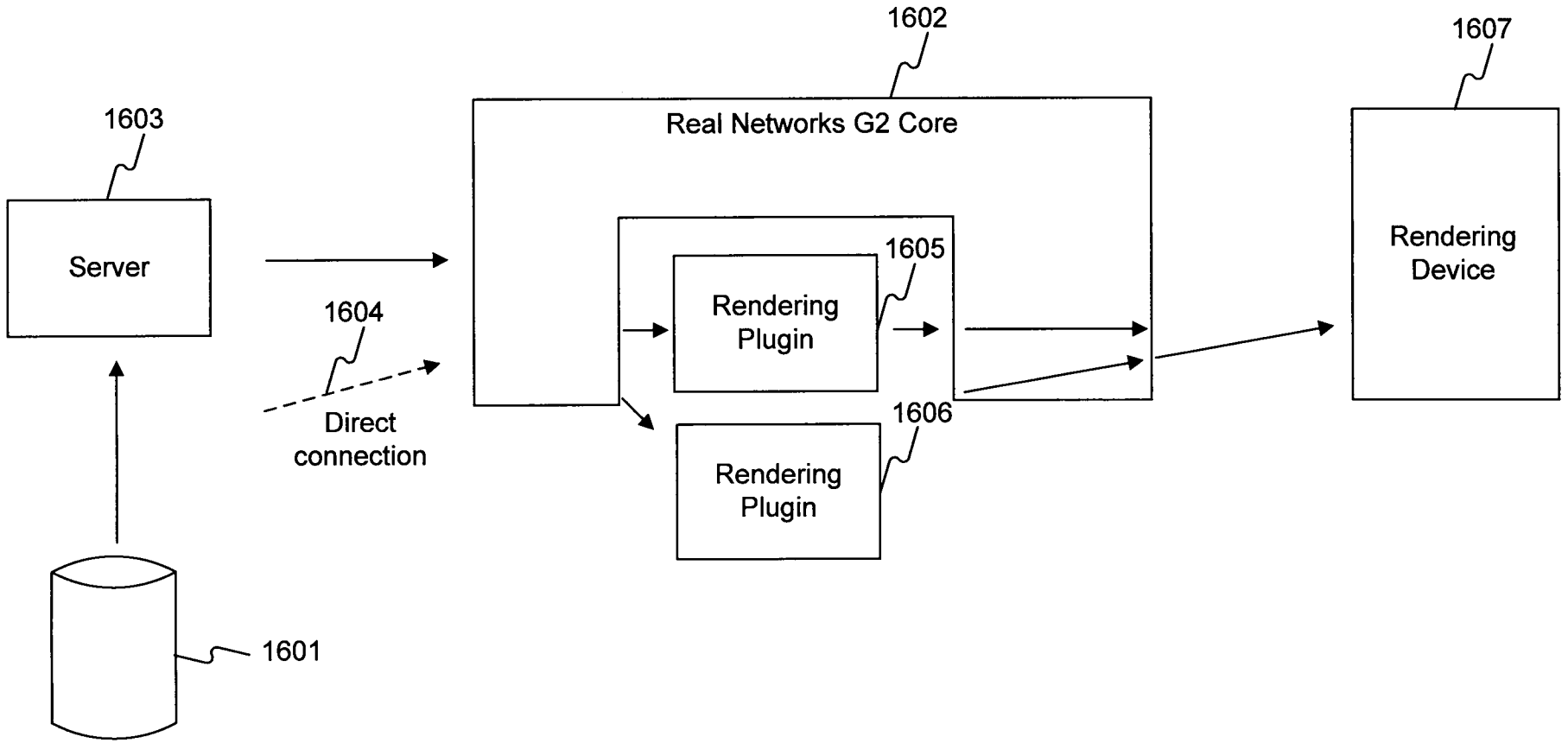

1602
1607
1603
Real Networks G2 Core
Server
1605
Rendering
Plugin
Rendering
Device
1604
Direct
connection
1606
Rendering
Plugin
1601

Fig. 16

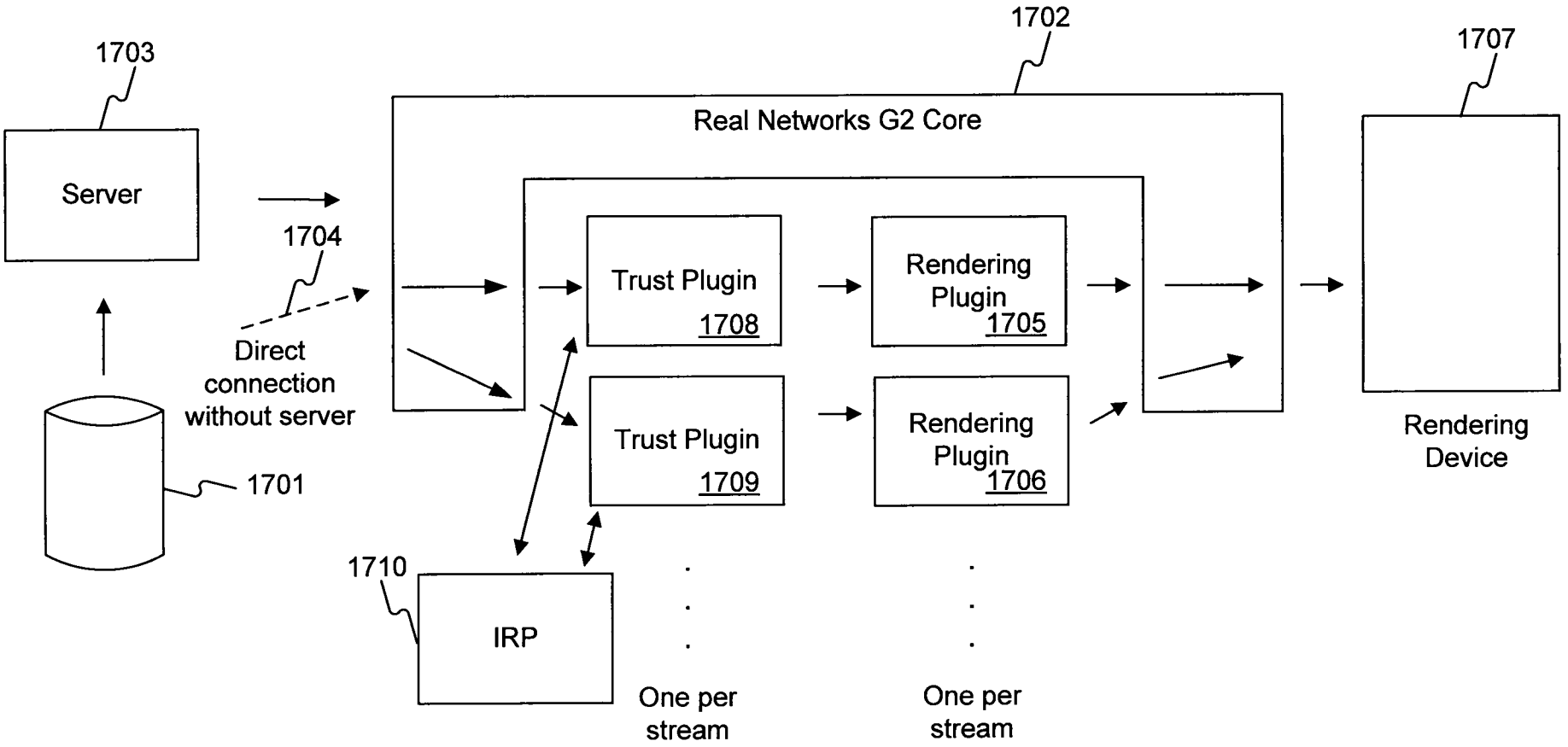

1703
Server
1704
Direct
connection
without server
1701
1702
Real Networks G2 Core
Trust Plugin
1708
Trust Plugin
1709
Rendering
Plugin
1705
Rendering
Plugin
1706
1707
Rendering
Device
1710
IRP
One per
stream
One per
stream

Fig. 17

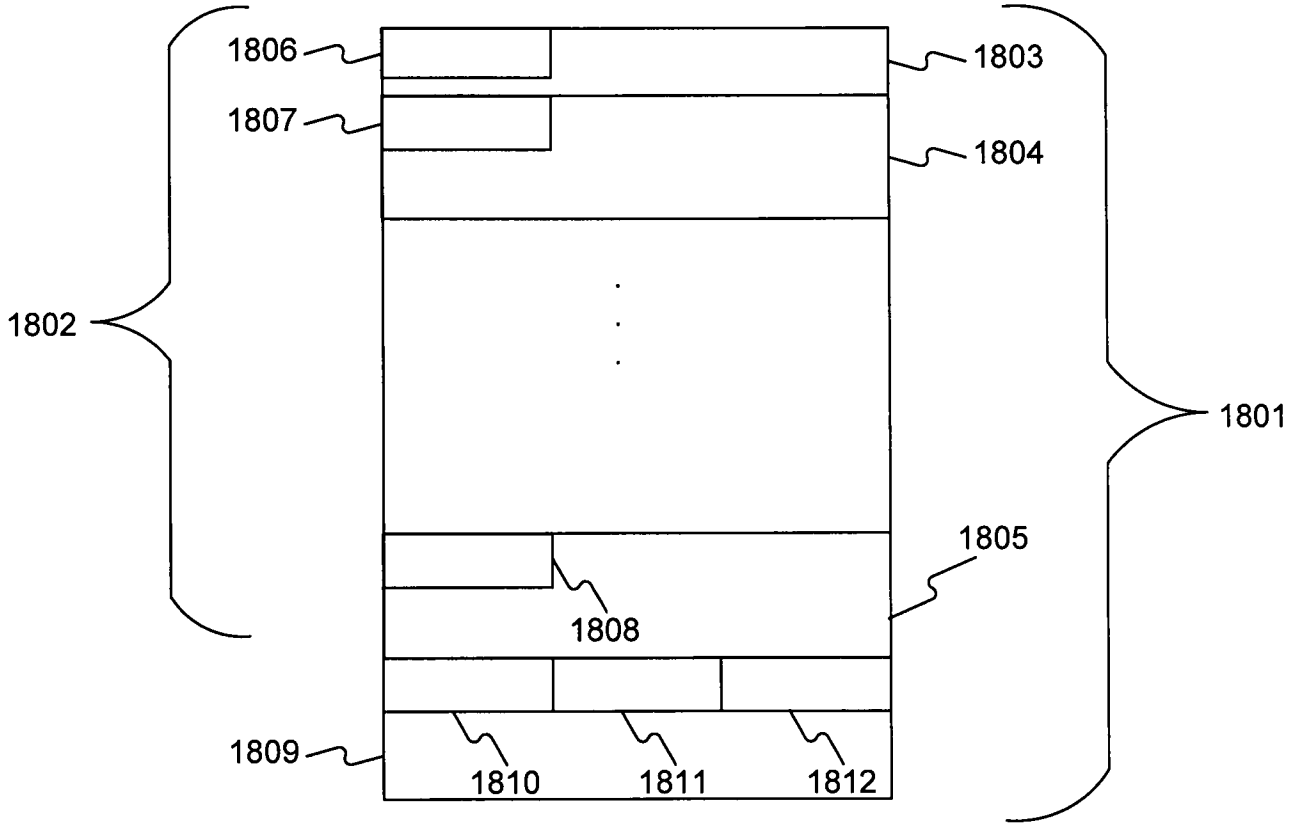
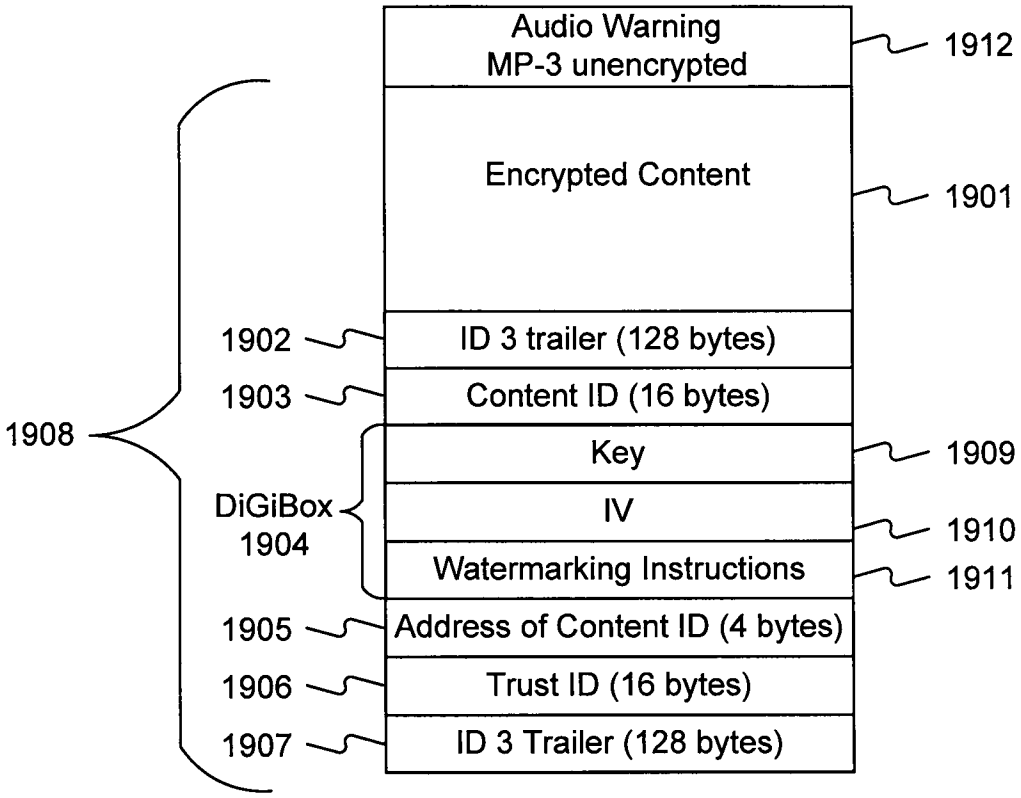



**Fig. 18**




**Protected MP3 Format**

**Fig. 19**

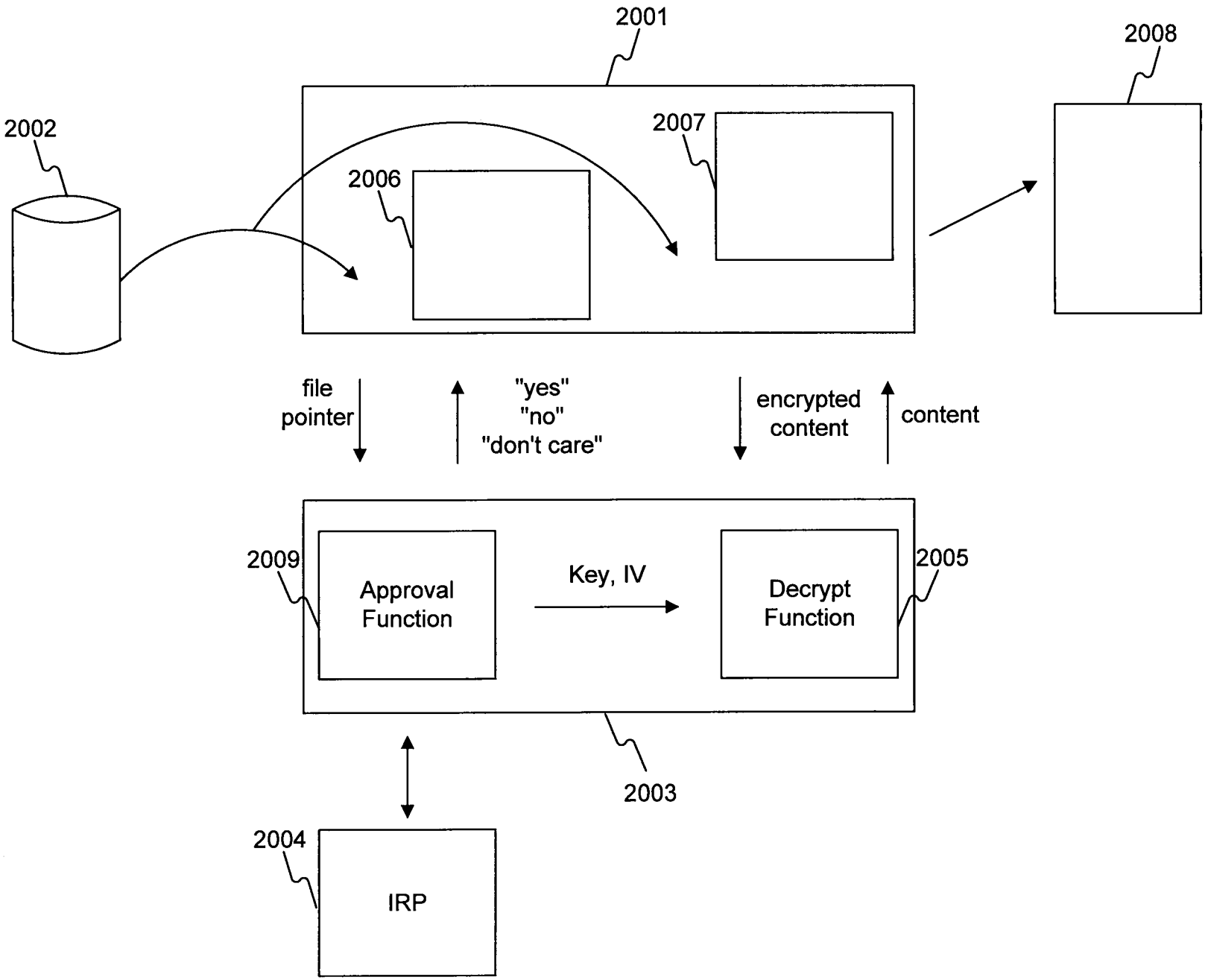

2001
2008
2002
2007
2006
file
pointer
"yes"
"no"
"don't care"
encrypted
content
content
2009
Approval
Function
Key, IV
Decrypt
Function
2005
2003
2004
IRP

Fig. 20

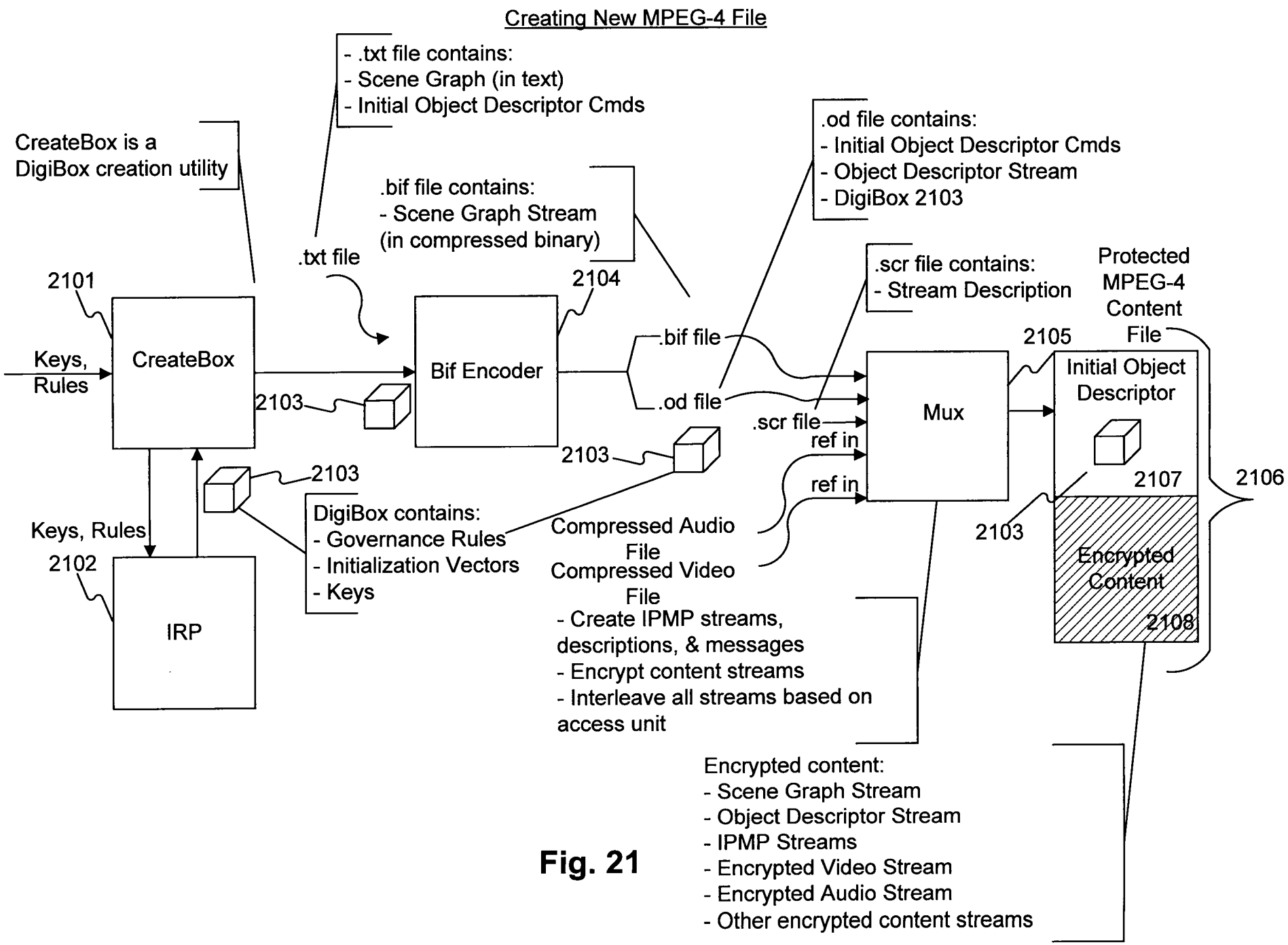

Creating New MPEG-4 File
- .txt file contains:
- Scene Graph (in text)
- Initial Object Descriptor Cmds
CreateBox is a
DigiBox creation utility
.bif file contains:
- Scene Graph Stream
(in compressed binary)
.od file contains:
- Initial Object Descriptor Cmds
- Object Descriptor Stream
- DigiBox 2103
.txt file
.scr file contains:
- Stream Description
Protected
MPEG-4
Content
File
2101
2104
2105
Keys,
Rules
CreateBox
Bif Encoder
.bif file
.od file
Mux
Initial Object
Descriptor
2103
.scr file
ref in
ref in
2107
2106
2103
2103
Keys, Rules
2102
DigiBox contains:
- Governance Rules
- Initialization Vectors
- Keys
Compressed Audio
File
Compressed Video
File
Encrypted
Content
2108
IRP
- Create IPMP streams,
descriptions, & messages
- Encrypt content streams
- Interleave all streams based on
access unit
Encrypted content:
- Scene Graph Stream
- Object Descriptor Stream
- IPMP Streams
- Encrypted Video Stream
- Encrypted Audio Stream
- Other encrypted content streams

**Fig. 21**

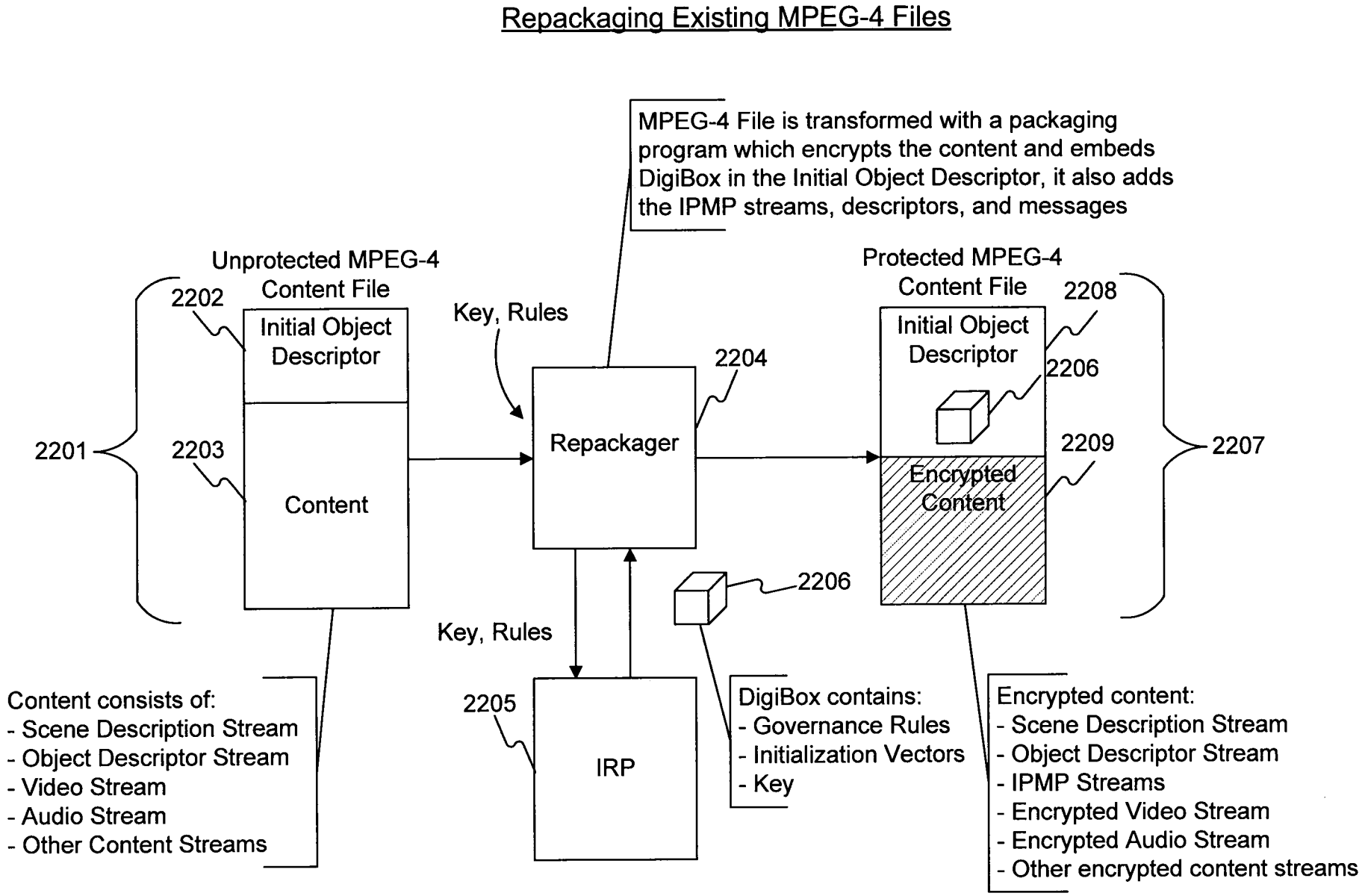

Repackaging Existing MPEG-4 Files
MPEG-4 File is transformed with a packaging program which encrypts the content and embeds DigiBox in the Initial Object Descriptor, it also adds the IPMP streams, descriptors, and messages
Unprotected MPEG-4 Content File
2202
Initial Object Descriptor
2203
Content
2201
Key, Rules
Repackager
2204
Protected MPEG-4 Content File
2208
Initial Object Descriptor
2206
2209
Encrypted Content
2207
2206
Key, Rules
2205
IRP
Content consists of:
- Scene Description Stream
- Object Descriptor Stream
- Video Stream
- Audio Stream
- Other Content Streams
DigiBox contains:
- Governance Rules
- Initialization Vectors
- Key
Encrypted content:
- Scene Description Stream
- Object Descriptor Stream
- IPMP Streams
- Encrypted Video Stream
- Encrypted Audio Stream
- Other encrypted content streams

**Fig. 22**

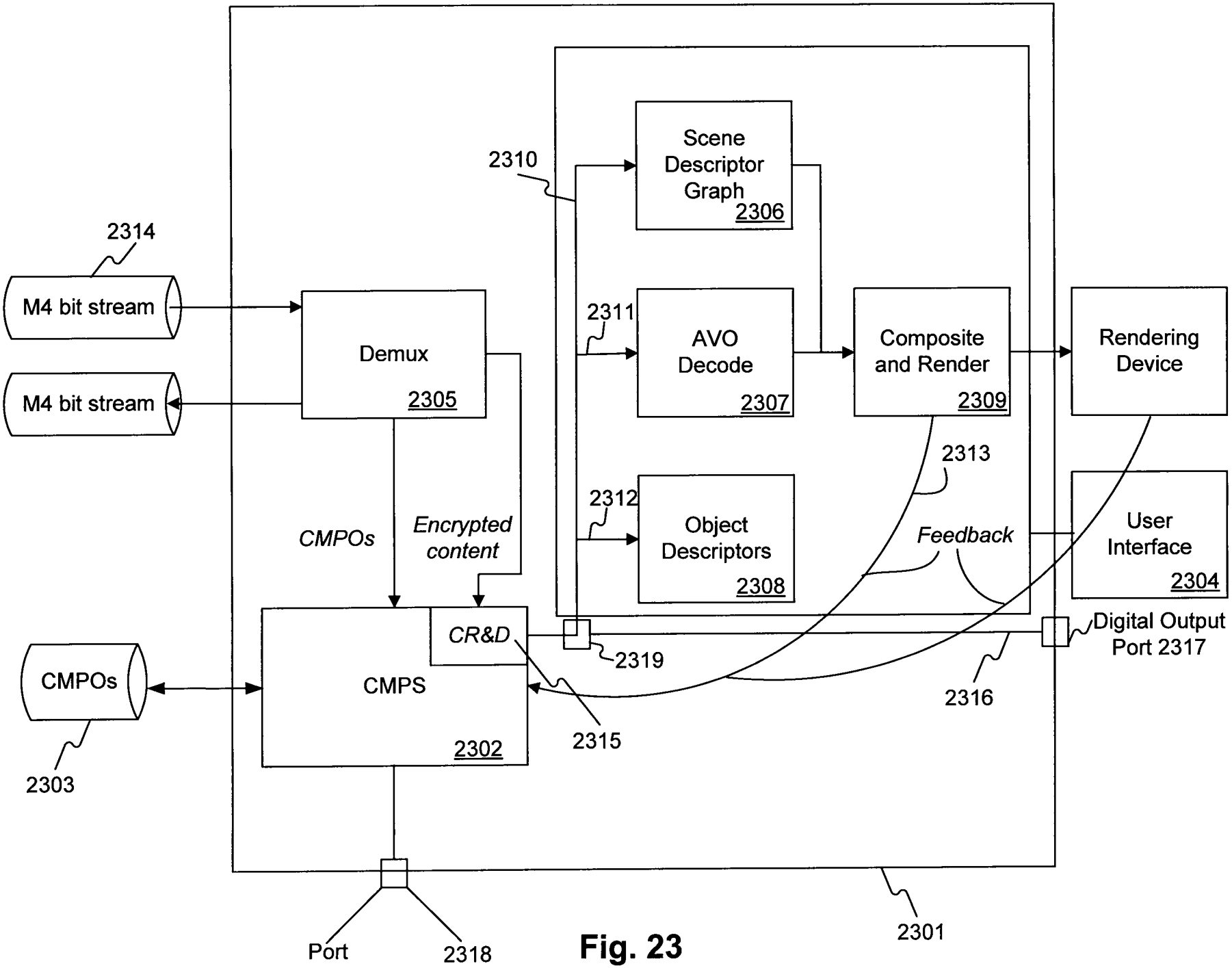

2310
Scene Descriptor Graph 2306
2314
M4 bit stream
M4 bit stream
Demux 2305
2311
AVO Decode 2307
Composite and Render 2309
Rendering Device
2313
2312
Object Descriptors 2308
CMPOs
Encrypted content
Feedback
User Interface 2304
CR&D
Digital Output Port 2317
2319
CMPOs
CMPS 2302
2316
2315
2303
Port
2318
2301

Fig. 23

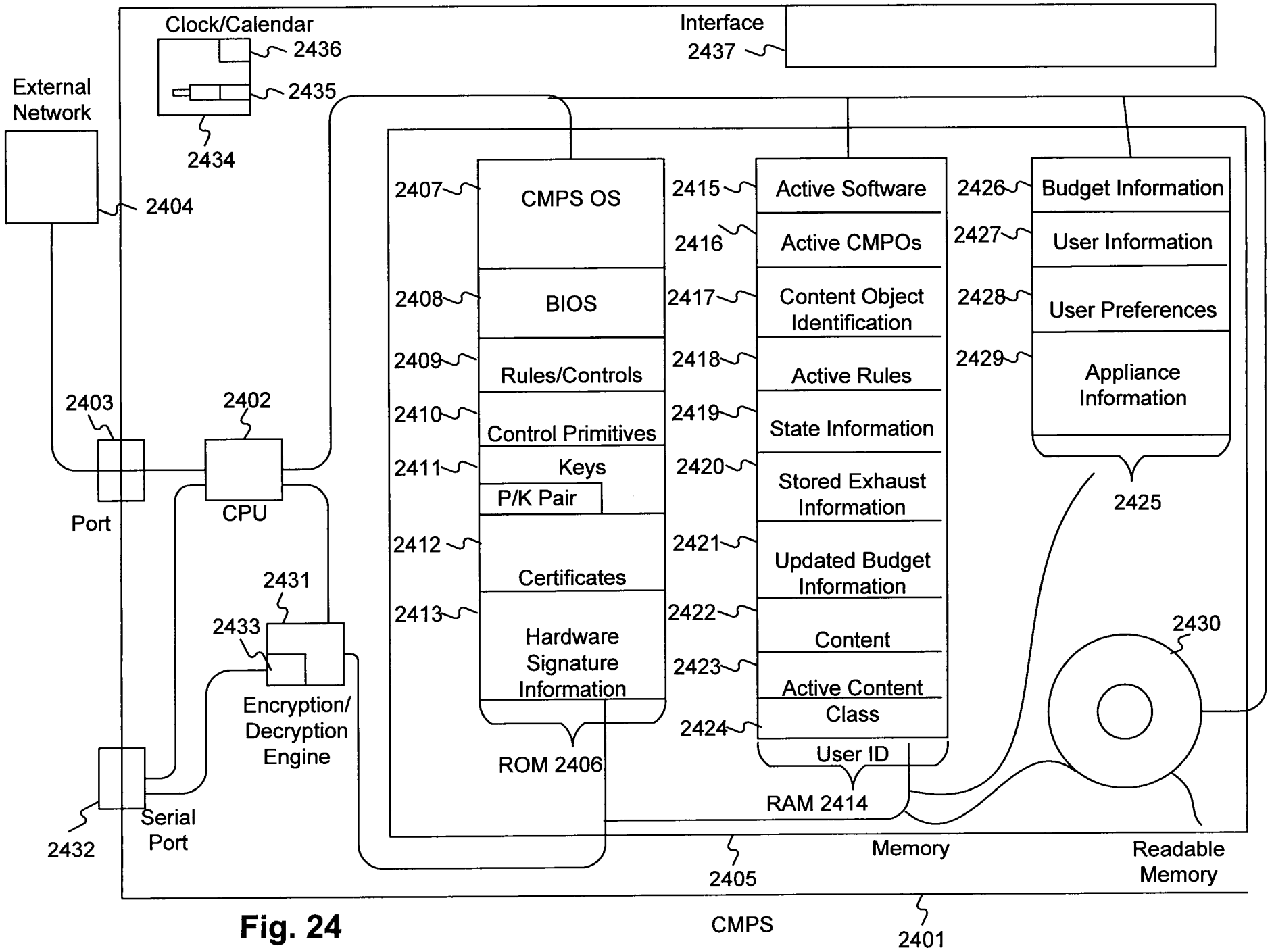
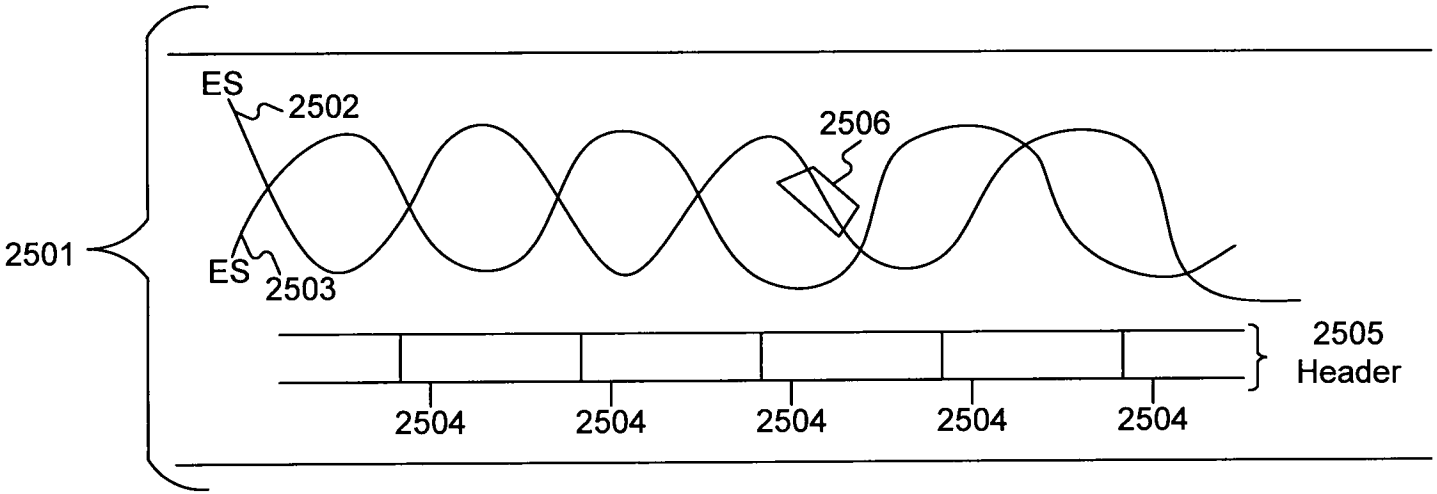

Clock/Calendar
2436
2435
2434
Interface
2437
External Network
2404
2403
2402
Port
CPU
2407
CMPS OS
2408
BIOS
2409
Rules/Controls
2410
Control Primitives
2411
Keys
P/K Pair
2412
Certificates
2413
Hardware Signature Information
ROM 2406
2415
Active Software
2416
Active CMPOs
2417
Content Object Identification
2418
Active Rules
2419
State Information
2420
Stored Exhaust Information
2421
Updated Budget Information
2422
Content
2423
Active Content Class
2424
User ID
RAM 2414
2426
Budget Information
2427
User Information
2428
User Preferences
2429
Appliance Information
2425
2430
2431
2433
Encryption/ Decryption Engine
2432
Serial Port
2405
Memory
Readable Memory
CMPS
2401

**Fig. 24**




Aggre_at_ Stream

**Fig. 25**

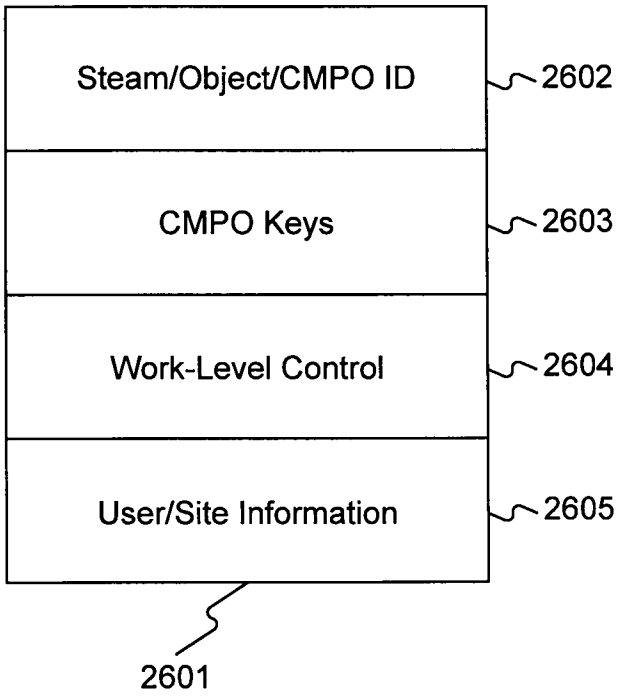

Steam/Object/CMPO ID
2602
CMPO Keys
2603
Work-Level Control
2604
User/Site Information
2605
2601

**Fig. 26**

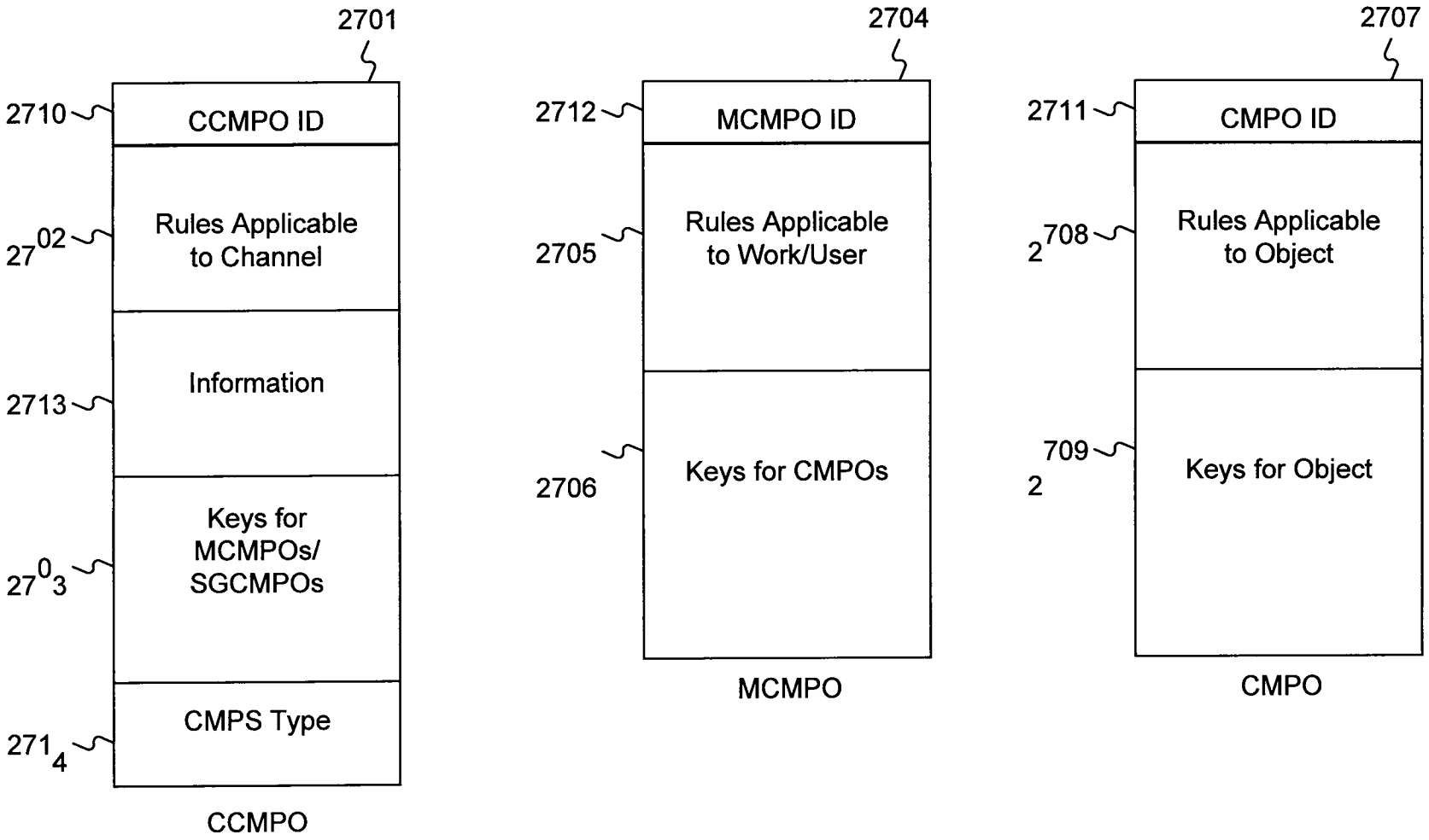

2701
2710
CCMPO ID
Rules Applicable to Channel
Information
Keys for MCMPOs/ SGCMPOs
CMPS Type
CCMPO
2704
2712
MCMPO ID
Rules Applicable to Work/User
Keys for CMPOs
MCMPO
2707
2711
CMPO ID
Rules Applicable to Object
Keys for Object
CMPO

**Fig. 27**

## CMPO Structure

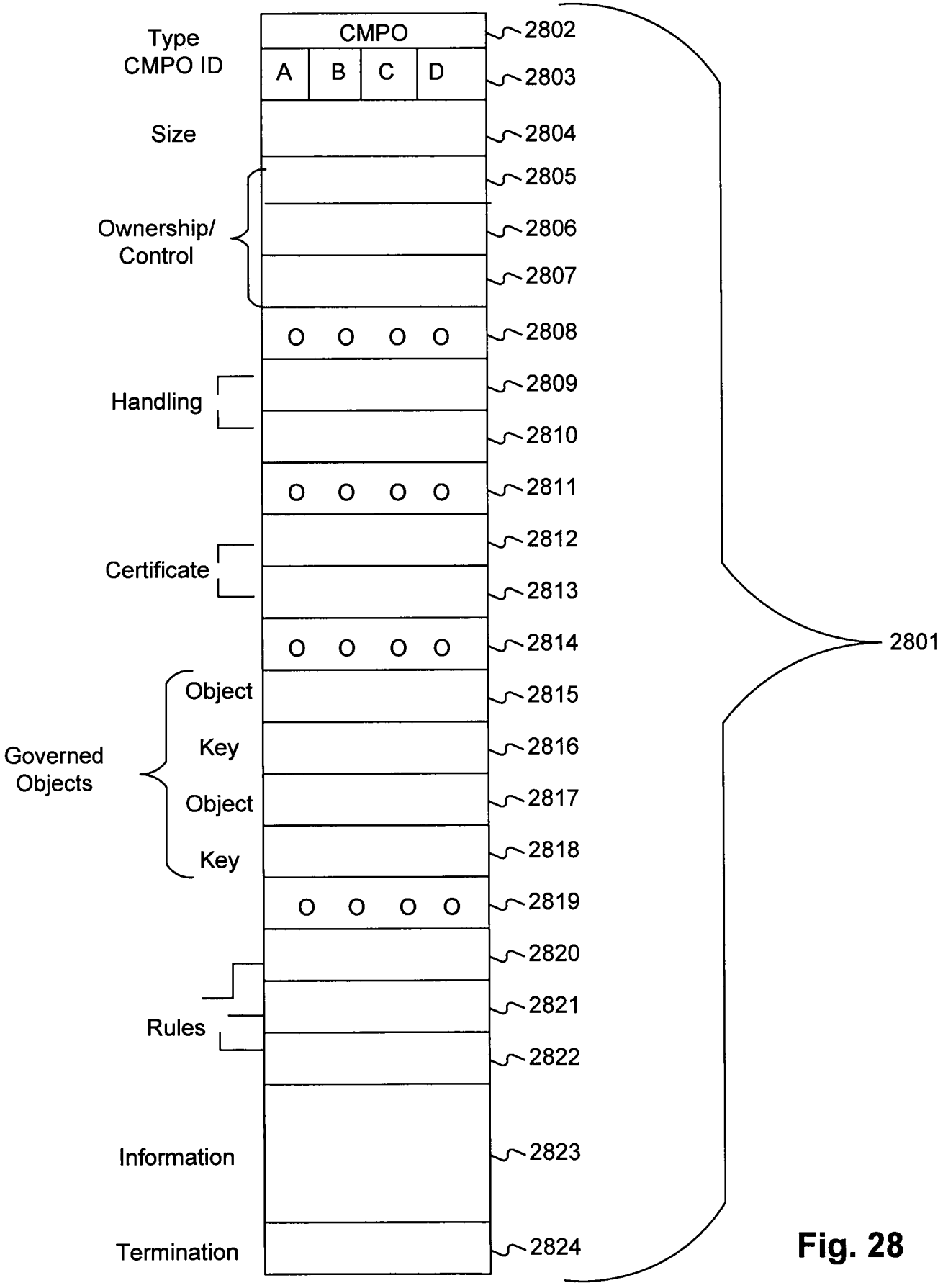



Fig. 28

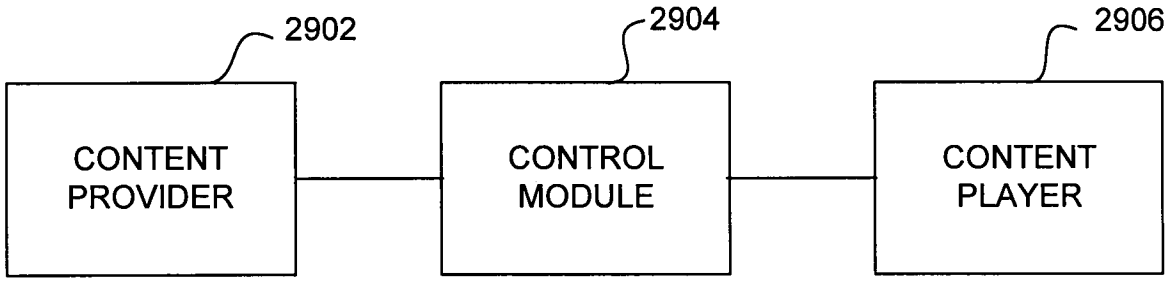

2902
2904
2906
CONTENT PROVIDER
CONTROL MODULE
CONTENT PLAYER

**Fig. 29**

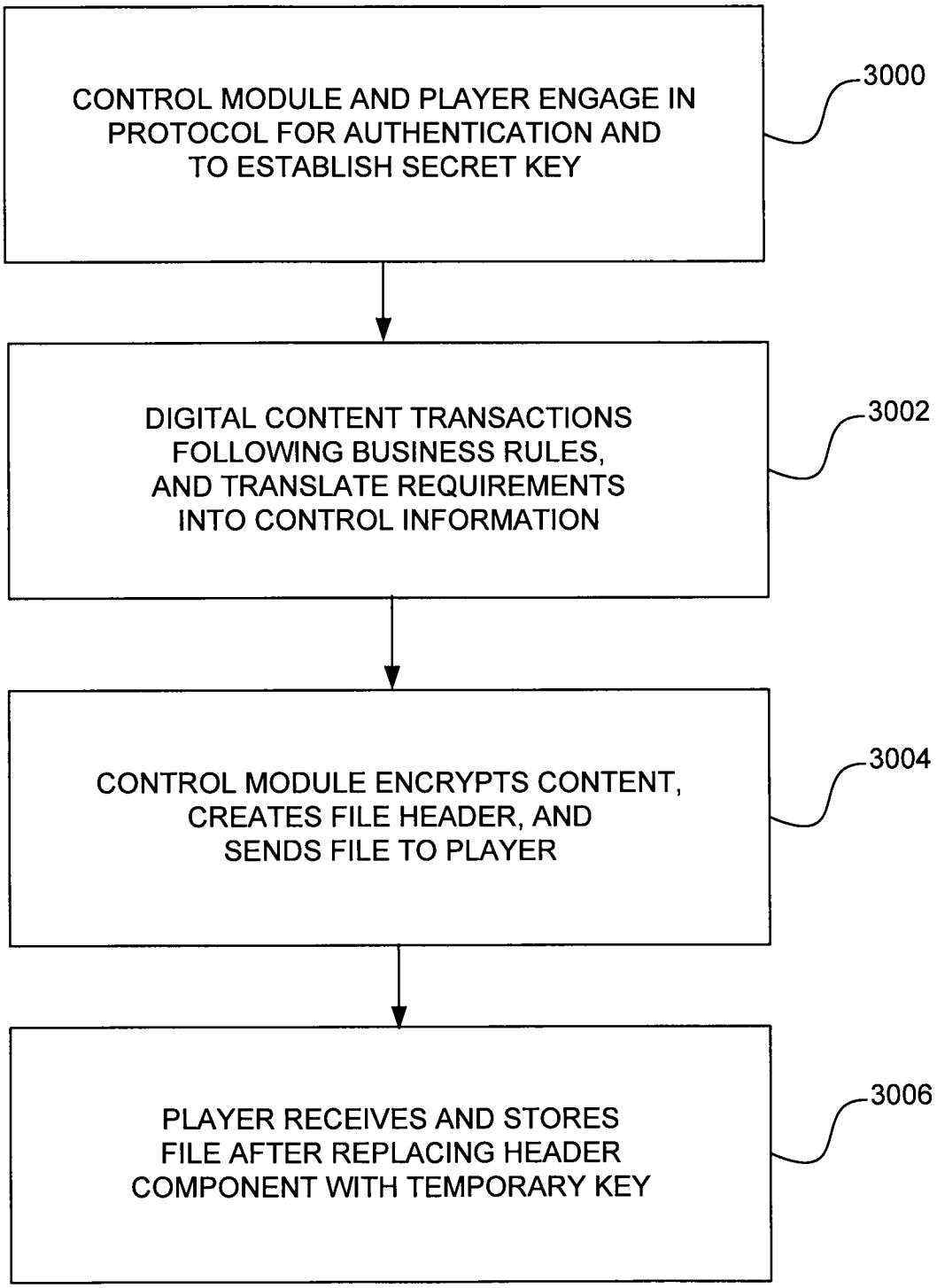

CONTROL MODULE AND PLAYER ENGAGE IN PROTOCOL FOR AUTHENTICATION AND TO ESTABLISH SECRET KEY
3000
DIGITAL CONTENT TRANSACTIONS FOLLOWING BUSINESS RULES, AND TRANSLATE REQUIREMENTS INTO CONTROL INFORMATION
3002
CONTROL MODULE ENCRYPTS CONTENT, CREATES FILE HEADER, AND SENDS FILE TO PLAYER
3004
PLAYER RECEIVES AND STORES FILE AFTER REPLACING HEADER COMPONENT WITH TEMPORARY KEY
3006

**Fig. 30**

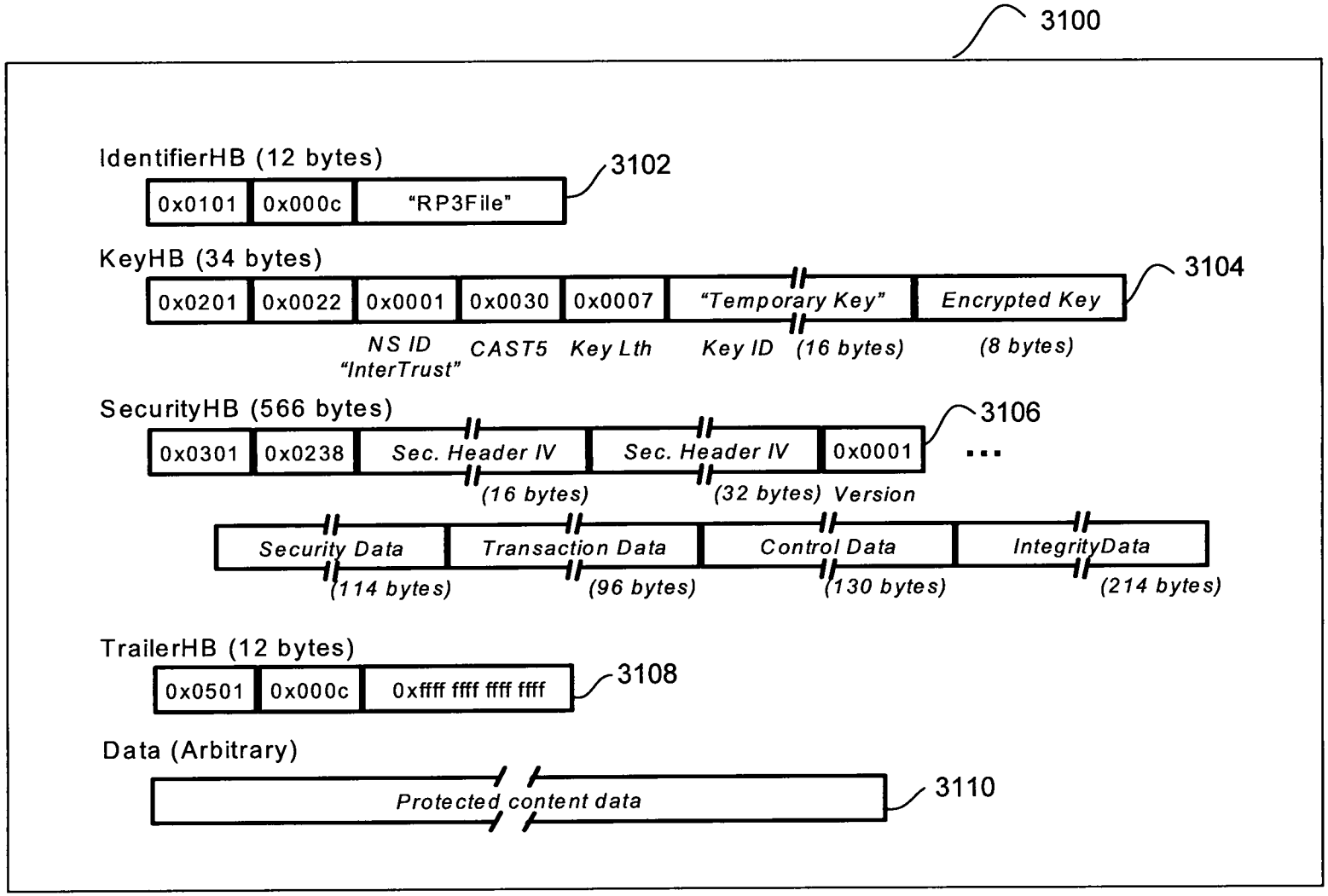

3100
IdentifierHB (12 bytes)
3102
0x0101
0x000c
"RP3File"
KeyHB (34 bytes)
3104
0x0201
0x0022
0x0001
0x0030
0x0007
"Temporary Key"
Encrypted Key
NS ID "InterTrust"
CAST5
Key Lth
Key ID
(16 bytes)
(8 bytes)
SecurityHB (566 bytes)
3106
0x0301
0x0238
Sec. Header IV
Sec. Header IV
0x0001
...
(16 bytes)
(32 bytes)
Version
Security Data
Transaction Data
Control Data
IntegrityData
(114 bytes)
(96 bytes)
(130 bytes)
(214 bytes)
TrailerHB (12 bytes)
3108
0x0501
0x000c
0xffff ffff ffff ffff
Data (Arbitrary)
3110
Protected content data

Fig. 31

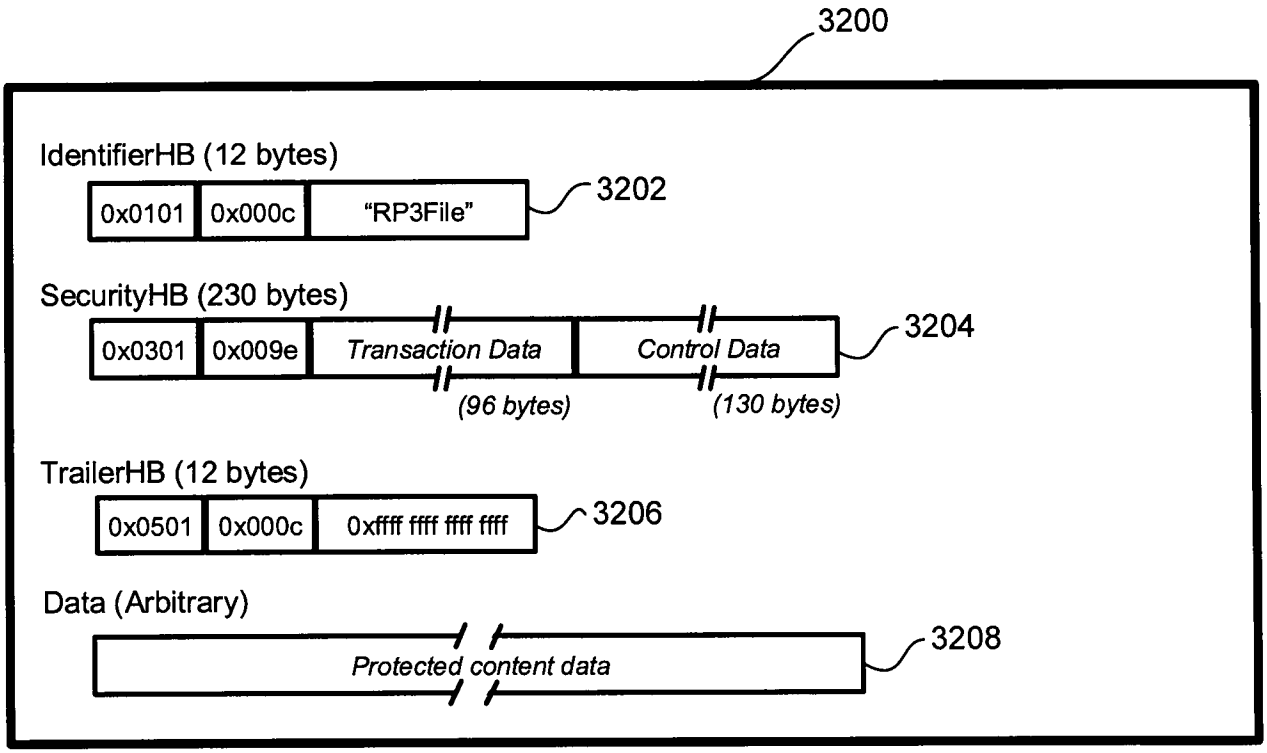

3200
IdentifierHB (12 bytes)
0x0101
0x000c
"RP3File"
3202
SecurityHB (230 bytes)
0x0301
0x009e
Transaction Data
Control Data
3204
(96 bytes)
(130 bytes)
TrailerHB (12 bytes)
0x0501
0x000c
0xffff ffff ffff ffff
3206
Data (Arbitrary)
Protected content data
3208

**Fig. 32**